Akademik Hassasiyetler **The Academic Elegance**
Yıl/Year: 2021 **Sayı/Issue: 17**
Cilt/Volume: 8 **Sayfa/Page: 369-399**
Araştırma Makalesi
Makale Gönderim Tarihi: 01/07/2021 **Makale Kabul Tarihi: 13/11/2021**

SİBER UZAMA YÖNELİK POLİTİK SÖYLEMDE İLETİŞİM GÜVENLİK YAKINSAMASI: ABD, AB VE TÜRKİYE ÖRNEĞİ[*]

Sevda ÜNAL[**]

Öz

Bu çalışmada risk ve tehdit kavramları temelinde ve güvenlik tedbirleri kapsamında siber uzama yönelik güvenlikleştirme olarak tanımlayabileceğimiz, gözetim, denetim ve kontrolü meşrulaştırma stratejilerinin ortaya çıkarılması amaçlanmaktadır. Güvenlikleştirmeye olanak sağlayan söylemsel stratejiler, siber uzamı düzenlemeye yönelik politika metinleri aracılığıyla inşa edilmektedir. Politika metinleri, resmî söylemin kamuya sunulma aracı olarak yönetimin eylemlerini meşrulaştıran ve yasallaştıran ideolojik bir pratiğe olanak sağlamaktadır. Politika metinleri aynı zamanda, hegemonyanın geliştirildiği, toplumun farklı sınıflarının sisteme dahil edildiği, dolayısıyla devletin meşruiyetinin ve devlete olan güvenin pekiştirildiği araç işlevi görmektedir. Bu kapsamda hazırlanan çalışmada, Türkiye, AB ve ABD siber güvenlik politika metinleri eleştirel söylem analizine tabi tutulmuştur. Norman Fairclough'un üç boyutlu eleştirel söylem analizinin izlendiği bu çalışmada, metinlerin "mezo düzey" analizine yer verilmiştir. Mezo düzey analiz, söylemsel temalar, stratejiler ve diğer metinlerle bağlantılarının ortaya çıkarılmasına olanak sağlamaktadır. Siber uzama yönelik düzenlemelerin kapsamının kişi hak ve özgürlüklerini ihlal edecek şekilde genişletilmesi dikkate alındığında, politika metinlerinin analizi, uzama yönelik kontrol, denetim ve gözetim faaliyetleri ve ideolojik pratikleri görünür kılmaktadır. Siber uzama yönelik düzenlemelerin ve tartışmaların güncelliğini koruması ve "güvenlik", "güvende olma" gibi çerçeveler altında gerçekleştirilen düzenlemelerin kapsamının kişi hak ve özgürlüklerini ihlal edecek şekilde genişletilmesi dikkate alındığında; bu çalışmanın siber uzama yönelik kontrol, denetim ve gözetim faaliyetlerinin tarihsel toplumsal bağlamını ve politika metinleri aracılığıyla görünmez kılınan ideolojik pratikleri görünür kılma açısından, özellikle iletişim çalışmaları alanında siber uzama yönelik çalışmalara katkı sağlayacağı değerlendirilmektedir.

Anahtar Kelimeler: *İletişim Çalışmaları, Siber Uzam, Siber Güvenlik, Güvenlikleştirme, Eleştirel Söylem Analizi.*

[*] Bu makale Ankara Üniversitesi Sosyal Bilimler Enstitüsü'nde, Prof. Dr. Funda Başaran Özdemir danışmanlığında tamamlanan "Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri" başlıklı yayımlanmamış doktora tezime dayanmaktadır.

[**] Dr. Öğr. Üyesi, Çukurova Üniversitesi, İletişim Fakültesi, Gazetecilik Bölümü, e-posta: sevdaunal@cu.edu.tr, https://orcid.org/ 0000-0003-2754-4780.

Önerilen Atıf: Ünal, S. (2021). Siber Uzama Yönelik Politik Söylemde İletişim Güvenlik Yakınsaması: ABD, AB ve Türkiye Örneği, *Akademik Hassasiyetler*, *8*(17), 369-399.

SECURITY-COMMUNICATION CONVERGENCE AT CYBER SPACE POLICY DISCOURSE: USA, EU AND TURKEY EXAMPLE

Abstract

This study aimed to reveal the strategies of legitimization of surveillance and control under the name of security measures for cyberspace, through the concepts of risk and threats. Discursive strategies that allow securitization are built through policy texts to regulate cyberspace. Policy texts are the means of publicizing official discourse and allow an ideological practice that legitimizes and legalizes the actions of the administration. Also, policy texts are the tools that the hegemony is developed, different classes of society are included in the system, and thus the legitimacy of the state and the trust in the state are reinforced. In this regard, the USA, EU, and Turkey's cybersecurity policy documents were subject to critical discourse analysis. In this study, critical discourse analysis method of Norman Fairclough was used and a meso-level analysis was performed. The Meso-level analysis makes it possible to reveal discursive themes, strategies, and their connections with other texts. Considering the widening of the scope of the regulations on cyberspace in a way that violates the rights and freedoms of individuals, analysis of policy texts makes visible control and surveillance activities and ideological practices. Considering that the regulations and discussions on cyberspace are kept up-to-date and the scope of the regulations made under the frameworks such as "security" and "being safe" is expanded in a way that violates the rights and freedoms of individuals; it is considered that this study will contribute to studies especially in the field of communication studies, in terms of making visible the historical social context of control and surveillance activities for cyberspace and ideological practices made invisible through policy texts.

Keywords: *Communication Studies, Cyber Space, Cyber Security, Securitization, Critical Discourse Analysis.*

Giriş

Enformasyon ve iletişim teknolojilerinde yaşanan gelişmeler, iletişimde zaman ve mekân sınırlamalarını ortadan kaldırmış; toplumların internet, kablosuz ağlar, cep telefonları ve diğer iletişim ortamları gibi yeni iletişim araç ve ortamlarıyla tanışmasına olanak sağlamıştır. Bu gelişmeler neticesinde, telekomünikasyon ve bilgi işlemlerin birleştirilmesi ve internet üzerinden her türlü veriyi (resim, kelime, ses) taşıma imkânı, uluslararası bilgi alışverişinde devrim yaratırken, yeni güvenlik tehditlerini de beraberinde getirmiştir.

Devletlerin iş yapış biçimleri de enformasyon ve iletişim teknolojilerindeki gelişmelerle değişmiştir. Bu teknolojiler olumlu etkileri ve yarattığı fırsatların yanında, gizlilik ve mahremiyet tartışmalarını da beraberinde getirmiştir. Devletlerin, siyasi etkisini ve ekonomik gücünü korumak için siber uzamı kontrol altına almaya yönelik girişimleri de belirginlik kazanmıştır. Güvenliğe ilişkin sorunlar ve kaygılar, siber uzamın güvenliğine yönelik yeni risk ve tehdit tanımlamaları, uzama yönelik denetim ve gözetim girişimlerini meşrulaştırma aracı olmuştur.

İletişim ve güvenlik çalışmaları farklı disiplinleri temsil etmekle birlikte, günümüzde iki alanın artan yakınsamasından söz etmek mümkündür Özellikle siber uzamı etkileyecek ve yine siber uzamdan kaynaklanan risk, tehlike ve tehdit kavramsallaştırmaları hem iletişim hem de güvenlik alanında ortaklığı gündeme getirmiş, yeni enformasyon ve iletişim teknolojilerinin ortaya çıkardığı bir dizi güvenlik tehdidi ve siber uzamda ortaya çıkabilecek çeşitli çatışma biçimleri analiz edilmeye başlanmıştır (Libicki, 2009:12). İletişim ve güvenlik çalışmaları arasındaki yakınsama, güvenlikle ilgili kurumların, teknolojilerin, politikaların ve programların oluşturulmasını ve meşrulaştırılmasını da etkilemiştir. 2001 yılında ikiz kulelere gerçekleştirilen terör saldırılarından sonra ABD liderliğindeki "terörle küresel savaş" anlayışıyla, enformasyon ve iletişim teknolojilerinin "güvenlikleştirme" adına gözetim, denetim ve kontrolü meşrulaştırılmıştır.

Bu kapsamda çalışmada, "risk" ve "tehdit" kavramları ekseninde, siber uzam için oluşturulan ve çalışmanın araştırma birimi olarak belirlenen politika metinleri aracılığıyla, güvenlikleştirme söyleminin inşa süreci, bu inşa sürecindeki söylemsel stratejilerin ortaya çıkarılması amaçlanmıştır. Güvenlikçi bir söylem inşa sürecinde uzama yönelik militarizasyon[1], denetim ve gözetim faaliyetlerinin meşrulaştırılması, kamu politikalarıyla etkileşim içinde ele alınmıştır.

Yönetimler tarafından oluşturulan politika metinleri, resmi söylemin kamuya sunulma aracıdır. Politika metinleri, resmi söylemi temsil ederek aslında yönetimin eylemlerini meşrulaştırmakta ve kamuoyunun eylemlere yönelik tepkisini şekillendirmektedir. Politika metinlerinin analiziyle yönetimin elini güçlendiren ve eylemlerini yasallaştıran ideolojik bir pratiğe tanıklık etme imkânı doğmaktadır (Jager, 2001: 34). Politika belgelerinin söylemi ve bürokratik dil, devletin, demokratik bir müzakere ortamında iş yaptığını kanıtlama aracıdır (Burton ve Carlen, 1979: 46). Resmi söylemler, hegemonyanın geliştirildiği, toplumun farklı sınıflarının sisteme dahil edildiği, dolayısıyla devletin meşruiyetinin ve devlete olan güvenin pekiştirildiği araçlardır. Böylece devletin denetim ve kontrol stratejileri desteklenmekte, meşrulaştırma aracılığıyla devletin keyfi eylemlerinden dolayı bozulan imajı onarılmakta ve özellikle sorunlu dönemlerde güven tazelenmektedir. Devlet mevcut kriz durumunun geçici olduğunu göstererek yeniden güven kazanmayı ve istikrarı sağlamayı amaçlamaktadır.

Bu kapsamda temel olarak çalışmada şu sorulara yanıt aranmıştır:

- Güvenlikleştirme söylemi siber uzamda nasıl bir inşa sürecinden geçmektedir? Bu süreç kişi hak ve özgürlüklerini nasıl etkilemektedir?
- Bu inşa sürecinde, ABD, Avrupa Birliği (AB) ve Türkiye örnekleminde, hangi söylemsel stratejiler uygulanmakta ve temalar öne çıkmaktadır?

[1] Militarizasyon veya militaristleşme "Askeri etkinin ekonomi ve sosyo-politik yaşam da dahil olmak üzere sivil alanlara uzanması" (Thee, 1977:296) olarak tanımlanmaktadır.

Çalışmada ABD, AB ile Türkiye'nin siber uzama yönelik politika metinleri incelenmiştir. ABD internetin doğduğu ülkedir. ABD bu keşfi hem uzam üzerinde hakimiyet sağlama amacıyla hem de dünya politikasına yön verme amacıyla kullanmaktadır. İnternet politika metinlerini oluşturma sürecinde ABD'nin temel söylemlerinden biri terörle mücadeledir. Bu kapsamda politika metinlerinin söylemi inşa edilmekte, kişi hak ve özgürlüklerinin sınırlandırılması meşrulaştırılmaktadır. Siyasi ve ekonomik bir örgütlenme olan AB ise ABD'den farklı olarak düzenlemelerinde insan hakları, gizlilik, mahremiyet gibi evrensel ilkeleri dikkat alan bir yaklaşım üzerinden ilerlemektedir. Türkiye ise politika yapım sürecinde hem terörle mücadele söyleminin, bu kapsamda kişi hak ve özgürlüklerine yönelik sınırlamaların öne çıktığı ABD metinlerinden faydalanmakta hem de AB uyum süreci kapsamında mevcut yasalarını AB mevzuatına göre düzenlemeye çalışmaktadır. AB uyum sürecinde bilgi toplumu altyapısını geliştirme ve politikalarını uyumlu hale getirmeyi hedefleyen Türkiye uzama yönelik düzenlemelerde AB politika metinlerini de dikkate almaktadır. Bu nedenle çalışmanın örneklemi ABD, AB ve Türkiye ile sınırlandırılmıştır. Örneklemin ABD, AB ve Türkiye ile sınırlandırılması çalışmanın sonuçlarının geçerliliğini olumsuz yönde etkilememektedir. Söylem analizinde örneklemin kapsamlı olması daha doğru sonuçlara ulaşılacağı anlamına gelmemektedir. Çünkü söylem analizinde seçilen örneklemin çalışmanın amacına uygun bir şekilde temsil niteliğine sahip olması ve seçilen metinlerdeki dil kullanımı önemlidir. Az sayıda metinden kapsamlı, tutarlı ve geçerli veriler elde edilebilmektedir. Hatta örneklemin gereksiz yere genişletilmesi analizi daha karmaşık ve çözümlenemez hale getirebilmektedir. Söylem analizinde araştırmanın amacı ve araştırma sorularının doğru bir şekilde kurgulanması, örneklemin büyüklüğünü ve temsil niteliğini etkileyen en önemli kriterler olarak kabul edilmektedir (Elliot, 1996: 66). Siber uzam politika metinlerinin analizinde Norman Fairclough'un eleştirel söylem analiz yöntemi temel alınmıştır.

Örneklem olarak seçilen politika metinlerinde benzerlikleri ve farklılıkları gösterebilmek için zaman zaman karşılaştırmalara başvurulmuştur. Ancak metinlerin aslında karşılaştırılabilir nitelikte olmaktan ziyade bir devamlılık içinde tasarlanması, yani birbirinden bağımsız olmamasından dolayı genel olarak karşılaştırmaya dayalı bir yöntem kullanılmamıştır.

Çalışma dört bölümden oluşmaktadır. İlk bölümde iletişim ve güvenlik çalışmalarının ortaklıkları "yakınsama" kavramı üzerinden açıklanarak, politik söylem, politika yapma süreci ve politika metinlerinin oluşumunda nasıl bir ortaklıktan söz edebileceğimiz tartışılmaktadır. İkinci bölümde, siber uzamın tanımı yapılmakta, uzama yönelik güvenlikleştirme söyleminin inşasında tarihsel-toplumsal bağlama ilişkin bilgi verilmektedir. Çalışmada kullanılan yönteme ilişkin bilgilerin bulunduğu üçüncü bölümde, Norman Fairclough'un üç boyutlu eleştirel söylem analizi ve çalışma esnasında yönteme ilişkin izlenen yol izah edilmektedir. Çalışmanın dördüncü ve son

bölümünde ise, Fairclough'un eleştirel söylem analizi çerçevesinde, politika metinlerinin mezo düzey analizi gerçekleştirilmektedir.

Siber uzama yönelik düzenlemelerin ve tartışmaların güncelliğini koruması ve "güvenlik", "güvende olma" gibi çerçeveler altında gerçekleştirilen düzenlemelerin kapsamının kişi hak ve özgürlüklerini ihlal edecek şekilde genişletilmesi dikkate alındığında; bu çalışmanın uzama yönelik kontrol, denetim ve gözetim faaliyetlerinin tarihsel toplumsal bağlamını ve politika metinleri aracılığıyla görünmez kılınan ideolojik pratikleri görünür kılma açısından, özellikle iletişim çalışmaları alanında siber uzama yönelik çalışmalara katkı sağlayacağı değerlendirilmektedir.

1. İLETİŞİM ÇALIŞMALARI VE GÜVENLİK SÖYLEMİ

Pek çok disiplinin birbirinden beslendiği günümüz sosyal bilimler ekosisteminde siber uzama yönelik politika inşasında ve bu inşa sürecini meşrulaştırmada iletişim çalışmaları ve güvenlik çalışmalarının yakınsaması önemli rol oynamaktadır. Bu yakınsama enformasyon ve iletişim teknolojilerinin gelişmesiyle günümüz politik, ekonomik, kültürel ve askeri faaliyetlerin alanı olarak beliren siber uzamın, devletlerin egemenlik ve hegemonya kurmada mücadele ettikleri bir alan haline gelmesinde tezahür etmektedir. Bu mücadele ve uzamda hâkimiyet kurma, devletin ve yurttaşın güvenliğini sağlama adına meşrulaştırılmaktadır. Bu meşrulaştırma mücadelesini sorgulama günümüzde hem iletişim çalışmaları ve hem de güvenlik çalışmalarının ortak ilgi alanıdır.

En basit şekilde tehlike ya da tehditlerden ve dolayısıyla bu tehlikelerin neden olacağı zararlardan kaçınma olarak tanımlayabileceğimiz güvenlik, karmaşık ve tartışmaya açık bir kavramdır. Güvenliğin amaçlanan sonuçları açısından en az üç farklı anlamı ayırt edilebilmektedir: İlk anlamda güvenlik, bir tehdidin yokluğu olarak görülebilmektedir. Bu anlamda önleyici güvenlik tedbirleri devreye girmektedir. Güvenliğin ikinci anlamı olası tehditlere karşı, tehdidin gerçeklemesini önlemek amacıyla caydırıcı tedbirlerin devreye girmesidir. Üçüncü anlamda ise amaç, gerçeğe dönüşen güvenlik tehdidi karşısında hayatta kalmak, güvenliğe yönelik tehdit gerçekleştiğinde bir çatışma veya felaketin etkilerinden korunmaktır (Krahmann, 2008: 381-382). Güvenlik kavramıyla ilgili önemli bir husus da kavramın anlamlandırılmasında içinde bulunulan toplumsal bağlamın etkisidir. Yani kavrama yüklenen anlam toplumsal bağlama göre farklılık gösterebilmektedir. Bu durum bize güvenlik kavramının "toplumsal inşa" olduğu gerçeğine götürmektedir. Böylece güvenliğe yüklenen anlam, hem gündelik hem de toplumsal yaşamı etkilemektedir.

Güvenlikleştirme de önceliklerin belirlenmesi, güce başvurma, yönetimin yetkilerinin genişletilmesi ve mevcut durumla baş edebilmek için diğer olağan dışı uygulama ve kararların meşrulaştırılması (Karam, 2005: 8) eylemlerinden oluşan bir süreçtir. Bu süreçte dikkat çeken husus, mevcut güvensizlik durumunu yönetmede nasıl bir yol izleneceği, kimlerin yetkilendirileceğidir. Bu süreçte alınan kararlar güvenlikleştirme söyleminin

sınırlarının çizilmesinde ve alınacak önlemler için kaynak sağlanmasında hayati öneme haizdir. Gerçekleşen güvenlikleştirme süreci 1980'lerden itibaren tanık olmaya başladığımız neoliberal yaklaşımı benimseyen toplumlarda riskleri yönetmenin temel yöntemlerinden biri olarak belirmektedir (Deisman, 2008: 21). Günümüzde ise güvenlikleştirme risk ve tehditleri yönetme gerekçesiyle enformasyon ve iletişim teknolojileri üzerinde hakimiyet kurabilmeye olanak sağlamaktadır (Neocleous, 2012: 11-12).

Siber uzamı güvenlikleştirmeye yönelik "önleyici müdahalelerin" 21. yüzyıldaki başlangıcına, ABD'de 11 Eylül 2001'de ikiz kuleler olarak adlandırılan Dünya Ticaret Merkezi'ne gerçekleştirilen terör saldırısına kadar götürülebilir. Bu saldırılardan sonra hem iletişim hem de güvenlik çalışmalarının giderek daha fazla ortak paydada buluştuğu görülmektedir. Böylece ulusal güvenlik anlayışının hakimiyet kazanmasıyla birlikte güvenlik devletine evrilinmektedir (Raab, 2005, 2012:4).

Güvenlik ve güvenlikleştirme çalışmalarında siber uzamın militarizasyonu ve böylece gözetim, denetim ve kontrolün meşrulaştırılması, bu süreçte yeni iletişim teknolojilerinin rolü iletişim çalışmalarının da alana dahil olmasını sağlamıştır. Özellikle yeni iletişim teknolojileriyle kritik altyapıların yakınsaması güvenliğe yönelik tehlike ve risk algısının inşasında etkili olmuştur. Siber uzamla bağlantılı ve gündelik hayatımızı etkileyecek teknolojilerin kritik altyapılar olarak ilan edilmesi, ticari kullanımına açılan internetin ağlaşmayla birlikte sürdürülebilir bir ekonomik düzeninin temel taşı olması, kritik altyapılara yönelik saldırı risklerinin ortaya çıkması siber uzamın güvenliğini ulusal güvenlik sorunu haline getirmiştir. Dolayısıyla siyasi gündemin ön sıralarına yerleştirmiştir. Bu noktada iletişim ve güvenlik çalışmalarının yakınsaması, güvenlik önlemleri ve bu önlemlerin meşrulaştırma sürecinde önemli bir yere sahiptir.

2. SİBER UZAMA YÖNELİK GÜVENLİKLEŞTİRME SÖYLEMİNİN İNŞASI

Siber uzama ilişkin tanımlamada sıklıkla karşılaşılan yanlışlardan biri de siber uzamın internetle aynı anlamda ele alınmasıdır (Klingova, 2013: 13). Bununla birlikte internet siber uzamın önemli ve hayati bir parçasını oluşturmaktadır. Siber uzama ilişkin farklı metinlerde farklı tanımlamalara rastlanmakla birlikte ABD tarafından yapılan tanım, uzamda hakimiyet kurması ve söz sahibi ülke olması açısından önem taşımaktadır. Siber uzam, 2009 yılında yayınlanan Siber Uzam Politika Değerlendirmesi'nde (President, U.S., 2009: 1) "İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve kritik sektörlerde bunların içine yerleşmiş denetleyicileri ve işlemcileri içeren, birbirine bağlı enformasyon teknolojileri altyapısı ağları" şeklinde tanımlanmaktadır. Siber uzamın yaygınlaşan anlamları arasında etkileşim ve sanal enformasyon ortamı da yer almaktadır. AB belgelerinde siber güvenliğin "ne"liğine ilişkin ifadelere rağmen siber uzamın net bir tanımı bulunmamaktadır. Türkiye'nin uzama ilişkin ilk strateji belgesi olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nda (Denizcilik, U. &

Bakanlığı, H., 2013: 2) "uzam" yerine "ortam" ya da "uzay" kavramları kullanılmakta ve siber uzam "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam" şeklinde tanımlanmaktadır. Bütün bu tanımlar dikkate alındığında interneti, bilgisayarların birbirleriyle bağlantı kurmasını sağlayan, yazılım ve donanım altyapısına sahip bir iletişim ağı yapılanması olarak tanımlamak mümkündür. Siber uzam ise, bilgisayar ağlarına ek olarak bu ağlara erişime sahip tüm veri kaynaklarını kapsamaktadır.

1970 ve 1980'li yıllar bilgisayarların ağlaşarak iletişime ve etkileşime olanak sağladığı yıllar olarak tanımlanabilmektedir. Bu yıllar bir yandan özgür iletişim ve etkileşim söylemini diğer yandan da denetim ve düzenleme alanına doğru evrilen tartışmaları beraberinde getirmiştir. Amerikalı hukukçu, İnternet ve Toplum Merkezi'nin kurucusu Lawrence Lessig, 1999 tarihli "Kod ve Siber Uzamın Diğer Yasaları" isimli çalışmasında, uzamın kod aracılığıyla düzenlemeye tabi tutulduğunu belirtmiştir (1999:83-84). Gözetim konusunda önemli çalışmalara sahip sosyolog David Lyon (2013:147) siber uzamdaki denetim ve düzenlemeye dikkat çekerek, uzama özgü bilgisayar ve ağ temelli gözetim, denetim ve düzenlemenin kod aracılığıyla gerçekleştirildiğini, bunun da deneyim olarak adlandırılabileceğini ifade etmektedir. ABD'li güvenlik uzmanları Richard Clarke ve Robert Knake (2011:44) de siber uzamı tanımlarken uzam aracılığıyla gerçekleştirilen kontrole vurgu yapmaktadırlar. Clarke ve Knake'e (2011:44) göre siber uzam, birbirine bağlı olan bütün bilgisayar ağları ve ağlar aracılığıyla kontrol edilebilen her şeydir.

Özellikle internetin kamunun kullanımına açılması ve ticari faaliyetlerin ağ üzerinden gerçekleştirilmeye başlamasıyla, 1990'lı yılların ortalarından itibaren, uzama yönelik güvenlik tedbirleri ulusal güvenlik tedbirleri kapsamında değerlendirmeye başlanmıştır. ABD'nin Oklahoma şehrinde 1995 yılında gerçekleştirilen bombalı saldırı ile 11 Eylül terör saldırıları, siber uzama yönelik güvenlik eksenli politikaların ortaya çıkışını kolaylaştırmıştır. Artık Soğuk Savaş sonrası dönemde geçerli olan tehdit ve dolayısıyla da tedbir tanımları değişmeye başlamış, tehdidin asimetrik niteliğinin artması ve siber uzamın yeni egemenlik alanı olarak ortaya çıkması askerî açıdan da tehlike, tehdit ve güvenlik kavramının siber uzamı da içine alacak şekilde genişlemesine yol açmıştır.

Siber uzam kavramı yaygınlaşmadan ve bu isimle düzenlemeler yapılmadan önce, 1997 yılında Bill Clinton'un ABD başkanlığı döneminde kritik altyapıların güvenliğine yönelik hukuksal düzenlemeler yapılmıştır. 11 Eylül 2001 terör saldırısını müteakiben kabul edilen Vatanseverlik Yasası ve yine 2003 yılında çıkarılan Siber Uzam Güvenliği Ulusal Strateji Metni ile siber uzam ve uzamla bağlantılı tüm teknolojiler, ulusal güvenliğin bir parçası haline gelmiş, istihbarat ve güvenlik birimleri uzama ilişkin faaliyetlere dahil olmuştur.

Aslında öncelikle bilgisayarlar, kritik altyapılar ardından da tüm uzamı kapsayacak şekilde genişletilen siber uzam kaynaklı risk ve tehdit söylemi, toplumsal yaşamın uzamla ilişkisi arttıkça daha fazla gündeme gelmeye

başlamıştır. Uzamın ekonomik, siyasi ve askeri potansiyeli uzam üzerinde egemenlik mücadelesini de artırmıştır. Pek çok ülkede "güvenlik" gerekçesiyle düzenleme, denetleme ve kontrol altına almaya yönelik söylem yaygınlaşmıştır (Cavelty, 2012: 141-142). Güvenlik açıklarından dolayı duyulan korku ve endişeyle beraber uzamın kontrolüne yönelik aceleci tavır uzamın "militarize" olmasının önünü açmıştır. Güvenlik tedbirleri resmi belgelerle yasallaştırılırken, yapılan düzenlemeler de kişi hak ve özgürlüklerine ilişkin kazanımda geriye gidişe neden olmuştur. Bunun başlıca nedeni ise uzama yönelik düzenlemede insanı temel alan bir yaklaşım yerine, devleti temel alan bir yaklaşımın öne çıkmasıdır.

3. YÖNTEM

Güvenlikleştirmeye giden yani devletlerin siber uzamda hegemonya tesis etme sürecinde meşrulaştırma, söylem aracılığıyla yani dil aracılığıyla gerçekleşmektedir. Ancak uzama yönelik bir güvenlikleştirme söylemi inşa pratiğinde, olguları sadece dile indirgemeyen, tarihsel toplumsal etkenleri de dikkate alan bir yaklaşım, politik sürecin doğru bir şekilde okunmasına olanak sağlamaktadır. Bu kapsamda çalışmada, siber uzama yönelik politika belgelerinin analizinde, eleştirel söylem analizi yöntem olarak belirlenmiştir. Eleştirel söylem analizinde her şey söylemle sınırlandırılmamaktadır. Söylem dışı etkenler de analize dahil edilmektedir. Toplumsal tarihsel bağlam, metinlerarasılık dikkate alınmakta, böylece dil-iktidar ilişkileri ve ideolojiler görünür hale getirilmektedir. Bu tür kaygılara Norman Fairclough'un eleştirel söylem analizinde yanıt bulmak mümkündür.

Fairclough'un üç boyutlu kavramsallaştırmasına dayalı eleştirel söylem analizimetin analizi (sözlü ya da yazılı), metnin üretim, dağıtım ve tüketim süreçlerinin yer aldığı söylem pratiği ile söyleme konu olayın toplumsal boyutunu bir bütün olarak içermektedir. Metin boyutunda dil incelenirken, söylem pratiği analizinde de bu pratiğin yükseldiği söylem çeşitleri sorgulanmaktadır. Toplumsal pratiklerin analizinde ise kurumsal ve organizasyonel boyutun söylemsel olaylarla etkileşimi irdelenmektedir. (Fairclough, 1992, 1-11; 1995:127,136, 229). Böylece Fairclough'u metin analizi (mikro), söylem pratiğinin analizi (mezo) ve toplumsal boyutun analizini (makro) birleştirir.

Fairglough'un eleştirel söylem analizinde, farklı siyasi etki alanları arasındaki söylem düzeni yapılanmasına odaklanarak, makro düzey bir çözümleme gerçekleştirilmektedir. Diğer iki düzey yani mezo ve mikro düzeyde ise, metin aracılığıyla çözümleme gerçekleştirilmektedir. Mezo düzeyde söyleme odaklanmanın yanında metnin mikro düzey analizi aracılığıyla diğer metinlerle bağlantısı kurulmaktadır. Bu özellik metinlerarasılık olarak adlandırılmaktadır (Fairclough, 1992:1-11; 2003:16; Mayasari, Darmayanti ve Riyanto, 2013:217-219). Daha çok yorumsayıcı olarak niteleyebileceğimiz metinlerarasılığın analizi, değişen ve dönüşen tartışmaları gösterirken, bu dönüşüm sürecinin nasıl gerçekleştiği konusunda ipucu vermektedir (Fairclough, 1992:101-123).

Doğası gereği polemiğe elverişli olan politika metinlerinin mezo düzey analizi, hegemonik ideolojilerin söylem ve tür karşılaşması aracılığıyla yayılmasını, sosyal ve ekonomik alanlarda yeniden yapılanan ilişkileri, eskinin yeni tarafından sömürülmesi gibi konuları ortaya çıkarmaktadır. Bunlar hem metnin uygulanmasında hem de söylemin düzeninde yani toplumsal uygulamalarda etkide bulunmaktadır. Diğer metinlere doğrudan ya da dolaylı yolla göndermede bulunan ve teknokratik bir dile sahip politika metinleri de metinlerarasıdır. Politika metinleri, metinlerarasılık özelliği ile tarihsel toplumsal bağlamı da ortaya çıkarmaktadır (Fairclough, 1992:85). Julia Kristeva'nın metinlerarasılık kavramına başvuran Lene Hansen, kavramı şöyle açıklamaktadır: "Metinler, diğer metinlerin içinde ve karşısında konumlanır, kimliklerini ve politikalarını oluştururken bu metinlerden faydalanırlar, geçmişten yararlandıkları kadar geçmişi gözden geçirerek düzeltirler, diğerlerini okuyarak ve diğerlerinden alıntı yaparak otorite kurarlar" (Hansen, 2006: 49). Eski metinlere gönderme yapılarak metin kendi meşruiyetini sağlamakta, aynı zamanda eskinin statüsünü yeniden inşa etmekte ve üretmektedir. Böylece karşılıklı bir meşruiyet üretilmekte ve anlam değişimi sağlanmaktadır (Hansen, 2006:49).

Politika metinlerinin analizi sadece metinlerarasılığı çözümleyerek değil söylemdeşliği de dikkate alarak gerçekleştirilmektedir (Fairclough, 1992:85). Söylemdeşlikle diğer söylem türleri ve metinler kastedilmektedir. Fairclough metnin söylemlerasılığını, metinlerarasılığının bir parçası olarak tanımlamaktadır. Bu kapsamda şu sorulara yanıt aranmaktadır: "Hangi türler, söylemler ve tarzlar kullanılmaktadır? Metne nasıl eklemlenmektedir?" (Fairclough, 2001: 124).

Çalışmada, ABD'nin 2009 yılından yayınlanan "Siber Uzam Politika Değerlendirmesi (Cyber Space Policy Review)", AB'nin 2013 yılında yayınlanan "Açık, Güvenli ve Emniyetli Bir Siber Alan (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)" başlıklı siber güvenlik stratejisi" ve Türkiye'nin 2013 yılında yayımlanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" analiz edilmiştir. Analiz edilen metinlerin seçiminde ve sınırlandırılmasında iki neden öne çıkmaktadır. Birincisi Türkiye'nin AB uyum süreci çerçevesinde yaptığı düzenlemelerde AB'nin hassasiyetlerini dikkate alması, aynı zamanda ABD'nin terörle mücadele yaklaşımındaki uygulamalarının Türkiye açısından önem taşımasıdır. İkinci neden ise, Türkiye dışındaki ülkelerin belgelerinin dillerinin anadilimizden farklı olmasının çözümleme açısından yarattığı zorluklardır. Barack Obama'nın başkanlığı döneminde yayınlanan politika belgesinin seçilmesinin temel nedeni, Obama'nın daha özgürlükçü ve eşitlikçi söylemiyle tanınmasına rağmen 2008 yılında seçim kampanyası sırasında siber uzamı "stratejik bir değer" olarak tanımlamasıdır. Bu tanımlama, siber uzama askeri müdahalenin önünü açarak güvenlikleştirme söylemine de meşruluk kazandırmıştır.

Bu kapsamda çalışmada politika metinlerinin mezo düzey analizinde metinlerdeki söylemsel temalar ortaya çıkarılmış, benzerlikler ve farklılıklar tartışılmıştır.

4. MEZO DÜZEY ANALİZ: SÖYLEMSEL ORTAKLIKLAR

Söylemsel ortaklıkları bulmaya yönelik mezo düzey bir analiz, hem makro hem de mikro yapıyla da bağlantı sağlamaktadır. Bu nedenle siber uzamı düzenlemeye yönelik politika metinlerinin analizinde söylemsel temalar, içinde bulunulan toplumun tarihsel sosyal bağlamından bağımsız ele alınamaz ve ortaya çıkarılamaz. Ayrıca uzamı düzenlemeye yönelik metinlerin türleri, tarzları ve söylemsel oluşumları dikkate alınmadan makro düzeyle de bağlantısı kurulamaz. Mezo düzey analiz, metinleri oluşturan söylem ve tarzları inceleyerek makro düzeyle bağlantı kurma, söylemlerarasılığı analiz etme ve böylece de örtük ideolojilerin ortaya çıkarılması olanağı sağlamaktadır. Söylemlerarası analizde metinde yer alan tema/temalar, temsil ettikleri ideoloji ortaya çıkarılmaktadır.

Analiz edilen politika metinlerde öne çıkan söylemsel temalar şunlardır:

- Teknolojik belirlenimcilik,
- Ulusal güvenlik tehdidi,
- Siber uzamın yönetişimi ve çok paydaşlılık,
- Risk yönetimi,
- Gözetim.

4.1. Teknolojik Belirlenimcilik

İnternetin kamunun kullanıma açılmasıyla hızla gündelik hayata nüfus etmesi ve iş yapış biçimlerini etkilemesi beraberinde teknolojik belirlenimcilik tartışmalarını da getirmiştir. Teknolojik belirlenimciliğe göre teknoloji toplumdaki temel değişim ve dönüşüm aracıdır. Teknolojik belirlenimcilik yaklaşımını eleştiren Raymond Williams (2003:12) teknolojinin içinde bulunduğu politik, ekonomik ve kültürel çevreden bağımsız değerlendirilmemesi gerektiğini ifade etmektedir. Teknolojik belirlenimciliğe dayalı yaklaşımlar iyimser ya da kötümser de olabilmektedir. İyimser yaklaşımlar teknolojinin olumlu yanlarına odaklanırken kötümser yaklaşımlar ise olumsuz etki ya da belirlenimci bakış açısıyla sonuçlarına odaklanmaktadır. Bu yaklaşımda temelde her şey tekniğe indirgenmiştir. Bu nedenle bu yaklaşıma göre gizlilik ve veri korumada yaşanan sıkıntılar teknik kaynaklıdır. Myriam Dunn Cavelty (2012:143) bu tür teknolojik belirlenimci bir yaklaşımı teknik söylem olarak adlandırmaktadır.

ABD, AB ve Türkiye özelinde incelenen politika metinlerinde de teknolojik belirlenimciliğe dayalı anlayışla karşılaşılmaktadır. Bu metinlerde gizliliğe ve verilerin güvenliğine yönelik tehditlerin enformasyon teknolojilerindeki açıklardan ya da kullanıcı pratiklerinden kaynaklandığı söylemi hakimdir. Böylece uzamda devletlerin gözetim ve denetim faaliyetleri, bilgilere izinsiz erişim meşrulaştırılmaktadır. Zihinlerde

güvenliğin ve gizliliğin teknoloji nedeniyle risk altında olduğu algısı oluşturularak kişi hak ve özgürlüklerinin aşındırılması meşrulaştırılmaktadır. Teknik söylemde siber uzam, hem uzamın mimari ve teknik yapısı hem de kullanıcıların teknik altyapısının üzerine yükselen karmaşık bir sosyo-teknik yapı olarak tanımlanmaktadır (Kabanov, 2014:7). Bu karmaşık yapıdan dolayı da ağlardan gelen tehditleri önlemede, sistem işleyişine yönelik müdahalelerle, sorunların çözülebileceği ifade edilmektedir (Bright, 2010:3). Metinlerde genel olarak teknoloji kullanımı ve teknolojinin getirileri olumlu bir şekilde aktarılmaktadır. Küresel ekonomiyi ağlar üzerinden dönüştüren, insanları zaman ve mekân gözetmeden birbirine bağlayan bu teknolojiler, bir saldırı gerçekleşene kadar işlevsel (Barnard- Wills, 2013:176) olarak tanımlanmaktadır.

ABD'nin 2009 yılında yayınlanan Siber Uzam Politika Değerlendirmesi'nde de teknoloji temel dönüştürücü araç olarak yansıtılmakta, bu da toplumsal bağlamın göz ardı edilmesine neden olmaktadır:

> "Siber uzam olarak bilinen, küresel olarak birbirine bağlı dijital bilgi ve iletişim altyapısı, modern toplumun hemen her yönünü desteklemekte ve ABD ekonomisi, sivil altyapı, kamu güvenliği ve ulusal güvenlik için kritik destek sağlamaktadır. Bilgi teknolojisi, küresel ekonomiyi dönüştürdü ve insanları ve pazarları asla hayal bile edilemeyecek şekilde birleştirdi" (President, U.S., 2009: 1).

Benzer şekilde AB tarafından yayınlanan 2013 yılı Avrupa Birliği Siber Güvenlik Stratejisi'nde siber uzam, enformasyon ve iletişim teknolojilerinin çatısı, aynı zamanda halihazırda ekonomik sektörlerin ağlaşmadan dolayı bağımlı olduğu kritik bir uzam olarak değerlendirilmektedir. Ayrıca gündelik hayatımızın, temel haklarımızın ve sosyal etkileşimimizin temeli olarak görülmektedir:

> "Günlük yaşamımız, temel haklarımız, sosyal etkileşimlerimiz ve ekonomilerimiz sorunsuz çalışan bilgi ve iletişim teknolojilerine bağlıdır." (JOIN/2013/01 final, 2013: 2).

Türkiye'nin strateji metninde ise uzamın güvende tutulması bilgi toplumu hedefini gerçekleştirebilmenin temel dayanağı olarak görülmektedir:

> "Bilginin gizlilik, bütünlük ve erişilebilirliğinin korunması olarak ifade edilen siber güvenlik; bilgi toplumuna dönüşmeyi hedefleyen ülkemizde, toplumun huzur ve refahı, ülkenin ekonomik kalkınması ve istikrarı, ulusal güvenliğin sağlanması gibi pek çok alanı etkileyen çok paydaşlı ve stratejik bir konudur." (Denizcilik, U., & Bakanlığı, H., 2013:17).

AB ile benzer şekilde Türkiye strateji metninde de "bilgi toplumu" vurgusu ön plandadır. Türkiye'nin bilgi toplumu stratejilerinde de teknolojik belirlenimci söylem hakimdir. Örneğin Serhat Çoban'ın (2013:1-7) Türkiye'nin 2006-2010 Bilgi Toplumu Stratejisi üzerine yaptığı çalışma da bu

savı doğrulamaktadır. Stratejide, teknolojiyi kullanan sayısı artışı ile toplumsal gelişme ve kalkınma doğru orantılı olarak sunulmaktadır.

4.2. Ulusal Güvenlik Tehdidi

Enformasyon ve iletişim teknolojilerindeki gelişme hızı ve bu teknolojilerin kötü amaçlı kullanım olasılığı, bu teknolojilerin neden olabileceği güvenlik sorunları konusunda bir tartışma başlatmıştır. Özellikle internetin toplumsal ve ekonomik etkisi ve yarattığı etkileşim de dikkate alındığında bu belirsizlik devletlere "ulusal güvenlik" gerekçesiyle güvenlik söylemi inşa etme olanağı sağlamaktadır. Soğuk Savaş'tan sonra dünyanın tek kutuplu hale gelmesiyle, toplumsal hayatın pek çok boyutunun entegre olduğu yeni bir alan olarak ve tehditlerin asimetrik bir yapıda olduğu siber uzam, ulusal güvenlik kaygıları ve güç çatışmaları üzerinden şekillendirilmeye çalışılmaktadır. ABD hegemonyasında bir siber uzam, ABD'nin teknolojik, ekonomik, askeri ve kültürel alanda üstünlüğünü sürdürmesine olanak sağlamaktadır (Lawson ve Gehl, 2011:1-19). Ulusal güvenlik açısından hangi ağın daha kritik önemde olduğu değişmekle birlikte, genel olarak devletin hem ekonomik hem de askeri ağlarda faaliyetini sürdürebilmesi için önceliğe sahip sistemler, iletişim altyapısı, ulaşım, bankacılık, su sistemleri, enerji, finans ve acil hizmetler olarak sıralanmaktadır (Powers ve Jablonski, 2015:175). Böylece ulusal güvenlik, uzama yönelik politika metinlerinde kritik altyapı güvenliği, siber güvenlik veyahut bilgi güvenliği adları altında enformasyon güvenliğini de içine alacak biçimde genişletilmiştir.

Ayrıca devlet merkezli bir düzenleme anlayışını kolaylaştıran tehdidin asimetrik niteliği internetin özgür ruhunu baltalamaya yönelik tedbir ve uygulamalarla sonuçlanmıştır. Bu uygulamalarla siber uzama yönelik denetim, gözetim ve kontrol söylemi hakimiyet kazanmıştır (Deibert ve Rohozinski, 2012:29). Ağlar aracılığıyla gerçekleştirilmesi kolaylaşan ve daha hızla küreselleşen terörle, çocuk pornosu, uyuşturucuyla ve kara para aklamayla mücadele (Assange, 2013:45) siber uzama devlet müdahalesinin diğer meşrulaştırma gerekçeleri olarak sıralanabilmektedir. Bu çerçevede alınan önlemler arasında, bir yanda uzam üzerindeki hareketliliğin ve veri akışının izlenmesi, denetlenmesi ve kaydedilmesi yer alırken, diğer yandan da uzamı askeri bir kompleks olarak değerlendirip askeri tedbirlerin artırılması yer almaktadır. ABD'de devletin güvenliği, kamu güvenliği, gizli bilgileri ve fikri mülkiyet haklarını koruma gerekçeleri kapsamında çeşitli kontrol araçları devreye sokulmuştur. Analize konu olan politika metinlerinde de görüldüğü üzere, siber uzam ABD, AB ve Türkiye'de ulusal, bölgesel ve uluslararası güvenliğin sağlanması ve sürdürülmesinde önemli bir ortam olarak ele alınmaktadır.

ABD Siber Uzam Politika Değerlendirmesi'nde siber uzam, ulusal güvenlik kapsamında ele alınmış, temel hak ve özgürlükleri kısıtlamaya yönelik maddelere yer verilmiştir. Önlemler diplomatik faaliyetler, ağ operasyonları, askeri ve istihbaratı faaliyetler olarak sıralanmaktadır. Hatta bu

önlemler meşrulaştırılmasında iletişimin devamlılığını sağlamanın amaçlandığı öne sürülmektedir:

> "Güvenlikle ilgili strateji, politika ve siber uzamdaki operasyonları kapsamakta ve tehdit azaltımı, güvenlik açığını azaltma, uluslararası düzlemde caydırıcılık, olaylara müdahale, kurtarma politikaları ve bilgisayar ağ işlemleri, bilgi güvencesi, kolluk, diplomasi, askeri ve istihbarat görevleri gibi faaliyetlerin tüm alanlarını kapsar." (President, U. S., 2009: i).

AB strateji metninde, üye ülkeler özelinde ulusal güvenlik kavramsallaştırması dikkat çekmekte; kritik altyapılara yönelik tehditler, siber suçla mücadele ve siber uzamın güvenliği öne çıkmaktadır. Uzamın güvenliği ve emniyeti *özgürlüğün* önkoşulu olarak sunulmaktadır. Özgürlüğün güvenlikle ilişkilendirilmesi ileriki dönemde "güvenlikleştirme" adı altıda yapılacak düzenlemeler meşruiyet sağlamaktadır:

> "Özgürlüğümüz ve refahımız, özel sektör inovasyonu ve sivil toplum büyümesini teşvik ederse gelişmeye devam edecek sağlam ve yenilikçi bir internete bağımlı. Ancak çevrimiçi özgürlük de güvenlik ve emniyet gerektirir." (JOIN/2013/01 final, 2013: 2).

Türkiye'de ise siber uzamın güvenliği "ulusal güvenlik" çerçevesine yerleştirilmekte, bu kapsamda uzamın korunmasında hem ulusal hem de uluslararası düzeyde "kolluk kuvvetleri" vurgusu öne çıkmaktadır:

> "Kurumlarımızın hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğimizin hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir." (Denizcilik, U., & Bakanlığı, H., 2013: 5).

> "Uluslararası işbirliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımı esas alınır." (Denizcilik, U., & Bakanlığı, H., 2013: 15).

ABD'nin politika metninde siber uzamı güvenlikleştirmeye yönelik söylem kamu nezdinde genel olarak kişi güvenliği, ulus güvenliği, kritik olarak adlandırılan altyapıların korunması, terör ve terörizmle mücadele ile sürdürülebilir ekonomi başlıkları altında ele alınabilecek söylemsel stratejiler aracılığıyla meşrulaştırılmaktadır (President, U.S., 2009). AB metninde ise, uzama herkesin kullanımına ve erişimine açık olması gereken ortak bir değer olarak yaklaşılmaktadır. Ulusal güvenlik kavramı AB üye devletleri nezdinde, enformasyon güvenliğini de kapsayacak biçimde "siber güvenlik, siber suç ve kritik altyapıların korunması" çerçevesinde ele alınmaktadır. AB'de temel haklar bir bütün olarak yani birbirinin tamamlayıcısı olarak değerlendirilmektedir (JOIN/2013/01 final, 2013).

4.3. Siber Uzamın Yönetişimi ve Çok Paydaşlılık

Uzamın ulusların ayrılmaz bir parçası haline geldiği günden bu yana en önemli sorunlardan biri de siber uzamda nasıl bir yönetim yapısı olacağı, kim ya da kimler tarafından yönetileceğidir. İnternetin dağıtık bir yapıya sahip olması, uzamın yönetimine ilişkin sorunların çözülememesindeki en önemli nedenlerden biridir. Bu nedenle çok taraflı ve tartışmalı bir alan olan siber uzamın yönetilmesinde "yönetişim" anlayışı öne çıkmaktadır.

Ağ yönetişimi hakkında çalışmaları bulunan Karen Banks (2005: 85) yönetişimi "Farklı çıkar gruplarının eşit koşullarda bir araya gelmesi, problemleri belirlemesi, çözümleri tanımlaması, politika geliştirme, uygulama, izleme ve değerlendirme, rol ve sorumluluklarında uzlaşılması" olarak tanımlamaktadır. Bu tanımda vurgulanan farklı çıkar gruplarının eşit koşullarda yönetimde yer alması anlayışının aksine 2005 yılında Tunus'ta gerçekleştirilen WSIS (Dünya Bilgi Toplumu Zirvesi)'de internet yönetişiminde devletlerin egemenliğine olanak sağlayan bir yaklaşım benimsendiği görülmektedir. Bu yaklaşım devlet dışı aktörlerin yönetişimde eşit şekilde temsil edilmesine engel olmaktadır. Ayrıca yönetişimde devlet dışında yer alan aktörlerin bazıları Dünya Telekomünikasyon Birliği (ITU) gibi ulus üstü kurumlar, özel sektör temsilcileri, internet hizmet sağlayıcılar, altyapı işletmecileri, teknik ve standart belirleme organları, hükümet dışı organizasyonlar (STK) vb.dir.

Çok paydaşlılığa ilişkin tartışmaların 2003 yılında başladığı görülmektedir. ABD internet yönetişimi için çok paydaşlı bir yaklaşımı benimsemekle birlikte (Powers ve Jablonski, 2015:24), çok paydaşlılığı aynı zamanda yapısal ve daimî eşitsizlikleri, gücün kötüye kullanımını vb. faaliyetleri görünmez kılmak için kullanmaktadır (Edmunds ve Wollenberg, 2001:232). Çok paydaşlılıkta amaç, farklı aktörlerin katılımıyla birlikte uzama yönelik ihtilaflı sorunları çözmektir. Ancak gerçekte ABD merkezli İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN), Dünya Çapında Ağ Konsorsiyumu (ISOC), İnternet Mühendislik Görev Gücü Mühendisleri (IETF) ve diğer çok paydaşlı organizasyonlar ABD lehine çalışmaya devam etmektedir (Powers ve Jablonski, 2015:24,135).

Hâlihazırda internet düzenlemesi, diğer devletlerin tüm itirazlarına rağmen ABD lehine bir yapıdadır. Mevcut çok paydaşlılık ABD şirketlerinin yönetişimde egemen olduğu bir yapıdır. Bu durum hem diğer devletler açısından eşitsiz bir ortamı temsil etmekte, hem de ABD'nin internet yönetişimindeki belirleyici konumunu sürdürmesine olanak sağlamaktadır. Ancak özellikle Edward Snowden'ın 2013 yılında ABD'nin siber uzamda yürüttüğü gözetim faaliyetlerini kamuya açıklamasıyla AB çok paydaşlı yönetişime verdiği desteği sorgulamaya başlamıştır (Bendiek, 2014:1).

ABD'nin hegemonik konumunu koruma isteği, politika metinlerinde de yansımasını bulmuştur. Siber uzamda karar verici olmayı, yönetişim politikalarını belirlemeyi sürdürme ve liderliğini koruma amacındadır. Böylece uzamdaki varlığını meşrulaştırmayı amaçlamaktadır. Aslında ABD metinlerindeki çok paydaşlılığa destek dili, ABD ve ABD şirketlerinin

uzamdaki belirleyiciliğini ve hâkimiyetini gizleme amacı da taşımaktadır (Manley, 2015, 10 Mart):

> "Devlet-pazar ilişkisi, korporatist bir yönetişim biçimini amaçlamaktadır. Telekomünikasyon, elektrik, enerji boru hatları, finansal ağlar ve diğer kritik altyapılar kinetik güç kullanmadan diğer devletlerden gelecek saldırılara karşı savunmasız olarak kabul edilir. Suç faaliyetlerinin 2008 yılı içinde bir trilyon değerinde fikri mülkiyet kaybına sebep olduğu değerlendirilmektedir. Kamu-özel ortaklığının ilk yönü 'kurumsal liderlik sorumluluğu' terimiyle ele alınır." (President, U.S., 2009: 28).

Çok paydaşlı yönetişimde amaç devlet ile özel sektör ve sivil toplum kuruluşlarıyla bilgi paylaşımı, kararlarda devlet dışındaki diğer aktörlerin de söz sahibi olmasıdır. Ancak ABD'nin politika değerlendirmesinde çok paydaşlılığı, kendisi ile aynı amaç ve düşüncede olan kurum ve kuruluşlarla işbirliği olarak tanımladığı görülmektedir:

> "Hükümet, kilit paydaşlarla birlikte çalışarak, hükümetten ve özel sektörden gelen bilgileri entegre eden ve bilinçli ve öncelikli güvenlik açığı azaltma çabalarına ve olay müdahale kararlarına temel teşkil eden gerçek bir ortak çalışma resmi elde etmek için etkili bir mekanizma tasarlamalıdır." (President, U.S., 2009: iii).

AB metninde ise çok paydaşlı yönetişim yaklaşımında ekonomik düzenin devamlılığı ve güvenliği ön planda tutulmuştur ve çok paydaşlı yönetişim desteklenmiştir:

> "Bilgi ve iletişim teknolojisi ekonomik büyümemizin bel kemiği haline gelmiştir ve tüm ekonomik sektörlerin güvendiği kritik bir kaynaktır." (JOIN/2013/01 final, 2013: 4).

> "AB, mevcut internet yönetişim modelindeki tüm paydaşların önemini yeniden teyit etmekte ve bu çok paydaşlı yönetişim yaklaşımını desteklemektedir." (JOIN/2013/01 final, 2013: 4).

Sivil toplum geleneği ve demokrasi söyleminin hâkimiyeti, AB metninde yaygın bir şekilde yer almakta, askeri önlemlere sınırlı şekilde yer verilmektedir. Ancak bu durum enformasyon ve iletişim teknolojilerinin güvenliğinin göz ardı edildiği anlamına da gelmemektedir. Gizlilik, bütünlük ve güvenilirlik ön plandadır; çok taraflı ve demokratik bir yönetişim anlayışı desteklenmektedir (JOIN/2013/01 final, 2013: 4):

> "Dijital dünya tek bir varlık tarafından kontrol edilmez. Şu anda birçoğu ticari ve sivil toplum kuruluşu olan ve İnternet kaynaklarının, protokollerinin ve standartlarının günlük yönetimine ve internetin gelecekteki gelişimine dâhil olan pek çok paydaş vardır. AB, mevcut internet yönetişim modelindeki tüm paydaşların önemini teyit eder ve bu çok paydaşlı yönetişim yaklaşımını destekler." (JOIN/2013/01 final, 2013: 4).

Türkiye'de yönetişim yaklaşımına uzamın güvenliğinin sağlanması aşamasında yer verilmektedir. Güvenliğin sağlanması ve sürdürülebilir olmasının çok paydaşlı bir yönetişim yapısıyla gerçekleştirilebileceğine dikkat çekilmektedir. Ancak strateji metninde yer alan ve uzama yönelik işbölümünün yer aldığı kısımda paydaşlar arasında devlet dışı aktörlere yeterince yer vermediği görülmektedir:

> "Siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğinin yanı sıra uluslararası iş birliği ve bilgi paylaşımı esas kabul edilir." (Denizcilik, U., & Bakanlığı, H., 2013: 15).

Çok paydaşlı yaklaşım ABD'nin küresel hegemonik çıkarlarıyla, AB'nin de ekonomik ve kültürel yayılmacılık amaçlarıyla ilişkilidir. Türkiye metninde ise çok paydaşlı model sürdürülebilir ekonomik refah çerçevesinde değerlendirilmektedir.

4.4. Risk Yönetimi

Tarih boyunca insanlar çeşitli risklerle karşı karşıya kalmıştır. İlk dönemlerde insanlar daha çok doğa kaynaklı risklerle karşılaşırken modern dönemle birlikte insanlar, doğada kendilerinin neden olduğu tahribat ya da sanayileşme kaynaklı teknolojik risklerle mücadele etmişlerdir. Günümüzde ise siber uzamın sağladığı ağlaşma üzerinde, "kritik" olarak atfedilen altyapıların çalışması, uzamın ekonominin, siyasetin ve toplumsal faaliyetlerin bir aracı haline gelmesi bir yandan hayatımızı kolaylaştırırken diğer yandan da yeni risk ve tehditleri de beraberinde getirmiştir. Bu risk ve tehditler tarih boyunca tanık olduğumuz gibi devletlerin güvenlik salama kapsamında gerçekleştirdikleri düzenlemelerin ve böylece iktidardakilerin meşruiyetlerini sağlamalarının bir aracı olmuştur. Risk ve tehdit kavramlarının tarihsel olarak izini süren ve devletlerin rolünü tartışan sosyolog Ulrich Beck (2006:229) güvenlik önlemlerini meşrulaştırma sürecini bir "ironi" olarak ele almaktadır. Çok çeşitleri olan bu ironin en yaygın olanı ve kolaylıkla benimseneni *terörizmle mücadele* söylemidir. Asimetrik bir tehdit olarak terör, devletlere güvenlik adına hak ve özgürlükleri kısıtlayabilmede önemli bir hareket alanı sağlamaktadır. Böylece açık ve özgür bir toplum yapısından uzaklaşılmakta, risk ve tehditler aracılığıyla hükümetler iktidarlarını sürdürülebilir kılmaktadır.

21. yüzyılın risk ve tehdit tanımları yapılarak güvenlik önlemleri adı altında denetim, gözetim ve kontrolün meşrulaştırıldığı bir alan olarak karşımıza çıkmaktadır siber uzam. Uzama yönelik güvenlik tedbirlerini savunanların temel argümanları da enformasyon toplumunun da risk toplumunun benzer özelliklerini taşımasıdır. Beck'e (2006:330-333) göre günümüz riskleri siyasi yorumlara açık risklerdir. Anthony Giddens'a (2000:38-47) göre ise de "imal edilmiş" risklerdir, bu nedenle daha tehlikelidir Güvenlikleştirme yaklaşımını savunanlar kritik altyapılar kaynaklı riskleri de

imal edilmiş risk kategorisinde gördükleri için tehlikeli olarak etiketlemektedirler (Bendrath, 2001:1).

Risk ve tehditler üzerinden güvenlik söyleminin inşa edildiği ve meşrulaştırıldığı siber uzama yönelik risklerde*, kritik altyapılara yönelik riskler, terör tehdidi ve siber suçlar* öne çıkmaktadır.

4.4.1. Kritik Altyapı Güvenliği

Bir nesneye kritiklik atfetme, bu nesnelerin uzun süre faaliyet dışı kalması durumunda yaşanacak kriz potansiyelinden kaynaklanmaktadır (Burgess, 2007:472-475). Uzama entegre altyapıların kritik olarak adlandırılması ve güvenlikleştirici söylemin hakimiyet kazanmasında altyapıların toplumsal yaşamın sürdürülebilirliği açısından hayati nitelikte olmasından kaynaklanmaktadır. Günümüzde enformasyon teknolojilerindeki artan yakınsama sayesinde pek çok ülkenin iletişim, sağlık, finans, enerji, su vb. altyapıları uzama entegre bir şekilde faaliyetine devam etmektedir. Bu da toplumsal yaşam açısından yeni güvenlik risklerine yol açmaktadır.

Başta ABD olmak üzere güvenlik adı altında militarist söylemin hâkim olduğu ülkelerde kritik altyapılar ulusal güvenliğin önemli bir parçası olarak değerlendirilmekte ve siber savaş söylemine meşruiyet kazandırılmaktadır. İnsan hak ve özgürlüklerinin ikinci plana itildiği bu yaklaşımlarda, devlet çıkarları dışındaki farklı güvenlik ihtiyaçları görmezden gelinmektedir (Cavelty, 2014:9-23).

> "Dijital altyapımız suçluların milyonlarca dolar çalması, diğer ulus devletlerin ve diğer işletmelerin fikri mülkiyet ve hassas askeri bilgi çalmasından dolayı hâlihazırda muzdariptir. Diğer izinsiz girişler kritik altyapı bölümlerine zarar verme tehdidi taşımaktadır. Bunlar ve diğer risklerin ulusun, ulusal güvenlik ve ekonomik çıkarların temelini oluşturan enformasyon sistemlerine güveni zayıflatma potansiyeli vardır." (President, U. S., 2009: i).

Ancak kritik altyapılar kaynaklı güvenlik sorunlarını geleneksel güvenlik anlayışı içinde değerlendirmek çok da doğru olmayan sonuçlar verebilmektedir. Bu tür bir yaklaşım kritik altyapıların büyük ekonomilerde daha dağıtık olduğu ve kendi kendini onarma yeteneğini sahip olduğu realitesinin gözden kaçırılmasına neden olmaktadır (Cavelty, 2008:1-2).

ABD'nin siber uzama yönelik militarist söyleminde ve bu söylemin meşrulaştırılmasında 11 Eylül terör saldırıları önemli bir yere sahiptir. Bu saldırılardan sonra kritik altyapılar, ulusal güvenlik açısından terör tehdidine karşı korunması gereken öncelikli alan olarak sunulmuştur. Daha sivil hak ve özgürlükleri gözeten bir söyleme sahip olmakla birlikte AB'nin de askeri önlemleri tamamen dışlamadığına dikkat çekmek gerekmektedir. 11 Eylül saldırıları, 2004 yılında Madrid'de, ardından 2005 yılında Londra'da gerçekleşen bombalı saldırılar, AB'nin kritik altyapılara yönelik politikasında değişikliğe giderek enerji ve altyapı trafiğine önem vermesine neden olmuştur (Ulmer, 2014:6). Böylece AB'de de "altyapılar"ı kritik olarak etiketleyerek güvenlikleştirme yönünde önemli bir adım atılmıştır. Altyapıların kritikliğine

vurgu özellikle ABD metinlerde yaygın olarak karşımıza çıkan söylemsel stratejilerdendir. ABD metninde terör tehdidi vurgusu öne çıkmakta, bu tehdide karşı alınacak yeni önemleri ve bu kapsamda ayrılan bütçenin arttırılmasını gerekçelendirebilmek için güvenlikçi bir söylem kullanılmaktadır:

> "Siber sistemlerimizin de dahil olduğu kritik altyapılarımıza yönelik hem fiziksel hem de siber saldırı kaynaklı önemli güvenlik açıklarını ortadan kaldırmak…" (President, U.S., 2009: 4).

> "ABD'nin bilgi ve iletişim altyapısına korumak, savunmak, saldırılara karşılık vermek, hasarları tespit etmek ve düzeltmeyi sağlamak…" (President, U.S., 2009: B-1).

> "Siber güvenlik politikası strateji, politika, siber uzamdaki operasyonlar ve siber uzam güvenliği ile ilgili standartları kapsamaktadır. Standartlar çok çeşitli olup tehdit azaltma, güvenlik açığı azaltma, caydırıcılık, uluslararası sorumluluk, olaylara müdahale, esneklik ve kurtarma politikası, bilgisayar ağ operasyonları, bilgi güvencesi, kolluk, diplomasi, askeri ve istihbarat misyonlarını kapsar. Bunlar küresel enformasyon ve iletişim altyapılarının güvenliği ve istikrarıyla ilgilidir." (President, U.S., 2009: 2)

AB güvenlik metninde, siber uzamla bağlantılı kritik altyapılar ve diğer hizmetler sıralanarak, bu hizmetlerin uzam kaynaklı risklerle karşı karşıya olduğuna dikkat çekilmektedir:

> "Bu düzenleme, enerji, ulaşım, bankacılık, borsalar ve kritik internet hizmetlerinin yanı sıra kamu idarelerinin etkinleştiricilerinin de aralarında bulunduğu kurumların karşılaştıkları siber güvenlik risklerini değerlendirmelerini, ağların ve bilgi sistemlerinin uygun risk yönetimi yoluyla güvenilir ve esnek olması ile bilgi paylaşımı sağlamayı amaçlamaktadır." (JOIN/2013/01 final, 2013: 6).

Ayrıca AB metninde kritik altyapıların korunmasında da daha *ılımlı* bir ifade kullanılarak sivil-asker işbirliği de desteklenmektedir:

> "Tehditlerin çok yönlü olduğu göz önüne alındığında, kritik siber varlıkların korunmasında sivil ve askeri yaklaşımlar arasındaki sinerjiler artırılmalıdır." (JOIN/2013/01 final, 2013: 11).

Türkiye düzenlemesine bakıldığında kritik altyapılar vurgusu öne çıkmakta, bu altyapılara yönelik saldırıların zararlarının yaratacağı etkinin büyüklüğünü tasvir etmede "kamu düzeni" ve "ulusal güvenlik" kavramlarına başvurulmaktadır:

> "Bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olabilecektir." (Denizcilik, U., & Bakanlığı, H., 2013: 1).

4.4.2. Terörizm ve Terörle Savaş

Terörle savaş ya da terörle mücadele, terör tehdidi, terörizm vb. ifadeler risk söyleminin önemli bir parçasıdır. Üzerinde uzlaşılmış net bir tanımı olmayan "terör", pek çok güvenlik uygulamasının meşrulaştırılmasında öne çıkan bir gerekçedir. Beck (2002: 43) terörizmi "dünya risk toplumu"nun vücut bulduğu bir olgu olarak ele almaktadır. Buna örnek olarak 11 Eylül saldırılarını göstermekte, bu saldırıyla birlikte "öngörülebilir riskten öngörülemeyen risk" dönemine geçtiğimizi de ifade etmektedir. Risk yaklaşımı, terörle mücadele etmede önemli faydalar sağlamakta ancak bu kapsamda alınacak önlemler ve nüfusun profilini oluşturma, gözetim, denetim vb. uygulamalar toplumsal yaşam açısından da önemli sorunları beraberinde getirmektedir.

Tehdit ve tehlikenin belirsizliği üzerine inşa edilen terörle mücadele söylemi, özellikle politika yapıcılar tarafından acil eylem gerektiren durum olarak tasvir edilmektedir. Ancak bu tehlikeler genelde objektif olmayıp yetkililer tarafından tanımlanmakta, dile getirilmekte ve böylece de toplumsal olarak inşa edilmektedir (Tsui, 2014:64-66). Gerçekliğin iktidar tarafından inşası ve yaygınlaştırılmasını Foucault (2002) şöyle açıklar: "…iktidar ilişkileri gerçek söylemin bir birikmesi, bir dolaşımı, bir işleyişi, bir üretimi olmaksızın ne işleyebilir ne yerleşebilir ne de ayırt edilebilir. Bu iktidar içerisinde, bu iktidardan yola çıkarak ve bu iktidar yoluyla işleyen belirli bir gerçeklik ekonomisi olmadan iktidar uygulaması olmaz. İktidar tarafından hakikat üretimine bağlı kılınırız ve ancak hakikat üretimi yoluyla iktidar uygulayabiliriz" (38). Fairclough (1995:42, 76) ideolojilerin doğallaşması görünmezliği ve otomatikleşmesini açıklamada Gramsci'nin "ortak duyu" kavramına başvurmaktadır. Ortak duyuyu "temel hegemonya stratejilerindendir" (Fiske, 2003: 225). Hegemonya " hegemonya, çoğunluğun kendisini ikincil konuma koyan sisteme rızasının sürekli biçimde kazanılmasını ve yeniden kazanılmasını içerir" (Fiske, 2003: 225). Terörle mücadele söylemiyle de savaş karşıtı, insan haklarına dayalı, çevre dostu, feminist ve küreselleşmeye karşı olmak gibi alternatif söylemler görünmez kılınmakta ve güvenlik eksenli bir söylem hegemonik hale gelmektedir (Jackson, 2005:19).

ABD güvenlik metninde terör vurgusu, ulusal güvenlik ve kamunun güvenliğine yönelik tehdit tanımında ve tehdidin inşasında yaygın bir şekilde kullanılmaktadır. Böylece terör tehdidi, ABD'nin siyasi gerçekliğini oluşturan ve terörle mücadele söylemini meşrulaştıran bir ortak duyu oluşturmaya hizmet etmektedir:

> "Teröristler ve uluslararası suç grupları gibi giderek büyüyen devlet ve devlet dışı aktörler ABD vatandaşlarını, ticareti, kritik altyapıyı ve hükümeti hedefliyor. Bu aktörler bilgiyi tehlikeye atabilir, çalabilir, değiştirebilir veya tamamen yok edebilir." (President, U.S., 2009: 1).

> "Özel mülkiyete ait kritik altyapıların silahlı saldırılara veya yabancı askeri güçlerin veya uluslararası teröristlerin fiziksel saldırıya veya sabotaja karşı

> ortak savunması Federal hükümetin temel sorumluluğudur. Benzer şekilde, hükümet bu altyapıları suçlulardan veya yerli teröristlerden korumada önemli bir rol oynamaktadır." (President, U.S., 2009: 28).

AB siber güvenlik metninde terör ve terör saldırıları ayrıca uzama yönelik saldırıları tanımlamada kullanılan *siber terör* kavramı, tehlike ve tehdidin boyutunu tasvir etmekte kullanılmaktadır:

> "Tehditler, doğal afetler ve kasıtsız hataların yanı sıra, cezai, siyasi olarak motive edilmiş, terörist veya devlet destekli saldırılar da dahil olmak üzere farklı kökenlere sahip olabilir." (JOIN/2013/01 final, 2013: 3).

Terörle mücadeleye artan vurgu ve bu kapsamda askeri iş birliği çağrısıyla daha demokratik anlayış, hak ve özgürlükler üzerine kurulu bir söyleme sahip olan AB'de de militarist bir söyleme doğru kayma olduğu görülmektedir. Bu değişim güvenlikleştirme sürecine doğru evrilen bir söylemin ipuçları olarak değerlendirilebilir.

Türkiye'nin siber güvenlik strateji ve eylem planında, siber uzama yönelik tehlikeler, kritik altyapı güvenliği ve ulusal güvenlikle ilişkilendirilmektedir. Türkiye metninde *terör* kavramı yer almamaktadır. Ancak metinde siber uzamın güvenliğinin ulusal güvenlik kapsamında değerlendirilmesi ve felaket senaryolarına yer verilmesi uzama yönelik güvenlikleştirme söyleminin inşasına yönelik adımlar olarak değerlendirilebilir. Bu adımlarla aslında askeri önlemlerin de önü açılmaktadır. Zaten Türkiye'nin strateji belgesinde, iş birliği yapılacak kurumlar arasında Millî Savunma Bakanlığı ve Genelkurmay Başkanlığının da yer alması, güvenlikleştirici söylemin inşa adımları olarak değerlendirilebilir:

> "Kritik altyapılara ait bilişim sistem ve verilerini hedef alan ısrarcı ve gelişmiş siber saldırıların kimler tarafından finanse ve organize edildiğinin tespiti ise neredeyse imkânsız görülmektedir. Bu durum ve özellikler siber ortamdaki risk ve tehditlerin asimetrik karakterini ortaya koymakta, mücadeleyi güçleştirmektedir." (Denizcilik, U., & Bakanlığı, H., 2013: 6).

> "Kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz olarak etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması." (Denizcilik, U., & Bakanlığı, H., 2013:13).

İncelenen üç düzenlemede de "siber güvenlik" ulusal güvenlik şemsiyesi altında değerlendirilmektedir. AB ve Türkiye'de güvenlikleştirme süreci henüz tamamlanmamıştır. ABD'de ise güvenlikleştirme yolunda önemli aşama kaydedilmiş olup militarist bir söylem ön plandadır.

4.5. Gözetim

Uzamın devlet kontrolü altına girmesi ile, bilgi akışının da kayıt ve kontrol altına gireceğini söylemek mümkündür. Başlangıçta bu kontrol ve

denetim ABD kamusu tarafından güvenlik önlemleri olarak doğal karşılanmıştır. Ancak eski CIA çalışanı Edward Snowden'ın, ABD Ulusal Güvenlik Ajansı (NSA)'nın ulusal güvenlik adına gerçekleştirdiği kitlesel gözetimin yurttaşlar açısından neden olacağı hak ihlallerini gözler önüne sermesi, merkezi hükümetin faaliyetlerine karşı tepkilere neden olmuştur. Artan sayıda devlet gözetim, denetim ve kontrol aracılığıyla yurttaşların uzamdaki faaliyetlerini kısıtlamaktadır. Siber uzamda egemenlik sağlama, totaliter rejimlerin gücü pekiştirme aracı haline gelmiştir. Ancak siber uzamda egemenlik isteğini sadece totaliter rejimlerle sınırlamak çok da gerçekçi olmamaktadır. Demokratik devletlerde de devlet gözetimini ve sansürü meşrulaştırıcı adımlar atılmış ve atılmaya devam edilmektedir (Deibert, 2013; Wagner 2014). Son yıllarda siber uzamda gözetim ve sansürün artışı, güvenlikleştirme söyleminin sonuçlarındandır. Özellikle 11 Eylül terör saldırılarının ardından demokratik ya da antidemokratik, totaliter, otoriter vb. nasıl tanımlanırsa tanımlansın pek çok ülkede siber uzamda gözetim yaygınlaşmıştır.

AB'de güvenlikleştirmeye yönelik adımlar atılsa da metinde "internet" herkesin kullanımına açık olması gereken ortak bir değer olarak görülmektedir. Ayrıca AB politika belgesinde internet kullanımının, başkalarına zarar vermeyi önleme dışında, hiçbir vatandaş için kısıtlanmaması gerektiği yönünde, normatif bir yaklaşımın özellikleri görülmektedir.

> "Temel hak ve özgürlükler Avrupa Birliği Temel Haklar Bildirgesi'nde benimsendiği/güvence altına alındığı şekle dayanırsa siber güvenlik etkili ve geçerli olabilir." (JOIN/2013/01 final, 2013: 4).

Ancak belgede üye devletlere ve Avrupa Savunma Ajansı'na (AB'nin askeri kanadı olarak değerlendirilmektedir) uzama yönelik tedbirlerde bir araya gelme çağrısında bulunulması, güvenlikleştirme adına atılmış önemli bir adım olarak değerlendirilebilir:

> "Üye Devletler ve Avrupa Savunma Ajansı işbirliği yapmalıdır. Bu kapsamda operasyonel AB siber savunma gereksinimlerini değerlendirerek AB siber savunma yeteneklerinin ve teknolojilerinin geliştirilmesini teşvik etmelidir. Dinamik risk yönetimi, gelişmiş tehdit analizi ve bilgi paylaşımı dahil olmak üzere AB siber savunma politika çerçevesini geliştirmelidir." (JOIN/2013/01 final, 2013: 11-12).

Türkiye metninde tasvir edilen yapılanma incelendiğinde yirmi dört saat çalışacak Ulusal Siber Olaylara Müdahale Merkezi'nin (USOME) kurulduğu ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulduğu görülmektedir. Olaylara müdahale konusu hem ABD ve AB, hem de Türkiye politika metninde yaygın olarak kullanılmaktadır. Bu durum kamuoyu tarafından Türkiye'de de kişi hak ve özgürlüklerine müdahale ve gözetim, takip ile denetimi meşrulaştırma olarak değerlendirilmiştir.

5. METİNLERARASILIK

Metinlerarasılık hem okumada hem de yazmada metnin diğer metinlerle, yazarlarla, okurlarla ilişkisine başvurmasıdır. Bu durum sözlü ya da yazılı metinlerin bir inşa olduğu ve bu süreçte metni anlamlandırırken, diğer metinlerle ilişkilerini de dikkate almamız gerektiğinin göstergesidir (Thibault, 1994:1751). Fairclough yeni metin inşa sürecinde önceki metinlerin ve türlerin, söylemsel uzlaşımların dikkate alınması gerektiğini ifade etmektedir. Aynı zamanda metinlerin tarihselliği ve heterojenliğine vurgu da metinlerarasılığın önemli bir özelliğidir (Fairclough, 1992: 102).

Politik metinlerdeki metinlerarasılığı sınıflandırırken Hansen (2006) "açık ve örtük" olmak metinlerarasılığı ikiye ayırmaktadır:

Tablo 1: Metinlerarasılık Türleri (Hansen, 2006: 51)

Metinlerarasılık	Metinlerarası Bağlantılar
Açık	Alıntılar
	Referanslar
Örtük	İkincil Kaynaklar
	Kavramsal
	Meşhur sözler, sloganlar

ABD ve AB siber uzam politika metinlerinde, söylemin inşasında tarihi metinlere ve diğer düzenlemelere dikkat çekilmektedir. Politik söylemin inşasında söz konusu ülkenin diğer politika metinlerine ya da diğer ülkelerin, akademisyenlerin, sivil toplum kuruluşlarının metinlerine başvurulmaktadır (Grewal, 2008:106-108). ABD ve AB'de yasa ve yönetmeliklere sıklıkla başvurulmakta, alıntılar ve referanslar yaygın şekilde kullanılmaktadır.

ABD politika metninde, siber uzamdan tam fayda saylayabilmenin kullanıcı bilgilerinin güvende olması, ekonominin işlediği altyapının güvende olması, kısacası kritik altyapıların güvende olmasıyla ilişkili olduğu belirtilmiş, bu kapsamda uzama yönelik güvenlik tedbirleri sıralanmıştır. Bu tedbirlerin gerekliliği daha önce iletişim teknolojileriyle ilgili yapılan yasal düzenlemelere referansla açıklanmıştır:

> "Teknolojinin ulusal ve ekonomik güvenlik ihtiyaçları üzerindeki etkisi Federal hükümetin yeni kanunlar ve kuruluşlar oluşturarak uyum sağlamasına yol açmıştır. Örneğin 1918 tarihli Ortak Karar'da Kongre, Başkan'a ABD'deki telgraf sisteminin kontrolünü üstlenme ve I. Dünya Savaşı sırasında gerektiği şekilde işletme yetkisi vermiştir. 1934 tarihli Haberleşme Kanunu Federal İletişim Yasası, Federal Radyo Komisyonu'ndan Federal İletişim Komisyonu'nu oluşturmuş ve kablolu ve radyo yayınları da dahil olmak üzere her türlü iletişim için geniş kapsamlı düzenleyici bir çerçeve kurulmuş ve o zamandan beri teknolojilerin gelişimini etkilemiştir." (President, U.S., 2009: 3).

Yukarıdaki alıntıda referans gösterilen Haberleşme Kanunu Federal İletişim Yasası aslında ABD Başkanlarına güvenlik adına denetim ve gözetimi tek elden gerçekleştirme olanağı sağlamıştır. Bu yasaya referans verilerek şimdi de yetkilerin tek elde yani ABD Başkanında toplanması gerektiği argümanı desteklenmektedir. Burada metinlerarasılık, daha önce yayınlanan politik metinlerden alıntı yaparak ya da o metinleri kaynak göstererek gerçekleştirilmektedir (Bazerman, 2003:86).

Enformasyon ve iletişim politikaları yerine güvenlik politikalarına ağırlık verilen, güvenliğin gizlilik ile kişi hak ve özgürlüklerinden önce geldiği ABD politika metninde, siber uzamın tanımı yapılırken de Ulusal Güvenlik 54/ Anavatan Güvenliği Başkanlık Direktifi 23'e (NSPD-54/HSDP-23) başvurulmuştur:

> "Güvenlikle ilgili strateji, politika ve siber uzamdaki operasyonları kapsamakta ve tehdit azaltımı, güvenlik açığını azaltma, uluslararası düzlemde caydırıcılık, olaylara müdahale, kurtarma politikaları ve bilgisayar ağ işlemleri, bilgi güvencesi, kolluk, diplomasi, askeri ve istihbarat görevleri gibi faaliyetlerin tüm alanlarını kapsar" (President, U. S., 2009: i).

ABD metninde fikri mülkiyet ve ekonomik rekabetin tartışıldığı "eylem durumu" bölümünde, 2008 yılı tarihli siber uzamla ilgili Başkanlık raporu yani ABD Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS) raporuna doğrudan referans verilmiştir. Yine siber uzam kaynaklı tehditler CSIS raporundakine benzer ifadeler ile tasvir edilmiştir (Lawson, 2013:173).

> "Dijital altyapımız suçluların milyonlarca dolar çalması, diğer ulus devletlerin ve diğer işletmelerin fikri mülkiyet ve hassas askeri bilgi çalmasından dolayı hâlihazırda muztariptir. Diğer izinsiz girişler kritik altyapı bölümlerine zarar verme tehdidi taşımaktadır. Bunlar ve diğer risklerin ulusun, ulusal güvenlik ve ekonomik çıkarların temelini oluşturan enformasyon sistemlerine güveni zayıflatma potansiyeli vardır." (President, U. S., 2009: i).

AB Siber Güvenlik Stratejisinde sorumluluk ulusal ve uluslararası olmak üzere uzamda faaliyet gösteren tüm aktörlere paylaştırılmıştır (JOIN/2013/01 final,2013: 15). Bu aktörler küresel bilgi toplumunun da aktörleridir. Ayrıca Ulusal Ağ ve Bilgi Güvenliği (NIS) politikasına metin boyunca referans verilmektedir. NIS, Avrupa Komisyonu tarafından geliştirilmiş olup, geçmiş düzenlemelere yapılan referanslardan AB'nin Bilgi Toplumu düzenlemelerinin devamı olarak değerlendirilebilir. NIS ile amaç kamu ve özel ağlar ile kaynakları korumak, siber uzamda karşılaşılabilecek sorunlarla mücadele etmektir (JOIN/2013/01 final,2013: 5).

Türkiye strateji metni incelendiğinde, bu metnin oluşturulma gerekçesi olarak Bakanlar Kurulunun 20 Ekim 2012 tarihli kararına referans verilmektedir

> "Bakanlar Kurulunca alınan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"

20 Ekim 2012 tarih ve 28447 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir." (Denizcilik, U., & Bakanlığı, H., 2013: 6).

Türkiye siber güvenlik stratejisinde "bilgi toplumu" hedefi referans alınmaktadır. Siber uzam güvenliği de bu hedefin bir parçasıdır. Türkiye'nin bilgi toplumu hedefine yönelik çalışmalarını yirminci yüzyılın sonuna kadar götürmek mümkündür. Bilgi toplumu hedefi çerçevesindeki bazı uygulamalar şöyle sıralanabilmektedir: E-dönüşüm Türkiye Projesi (2003), Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi (TÜBİTAK-2004), Bilgi Toplumu Stratejisi 2006-2010 (DPT-2004).

Sonuç

Siber uzamın ekonomik, politik ve toplumsal boyutu uzamın yeni bir egemenlik alanı olarak öne çıkmasına neden olmuştur. Devletler artık kara, hava ve deniz dışındaki güç savaşlarını siber uzama taşımışlardır. Ancak internetin önemli bir parçası olduğu uzam, bir yandan kamunun zaman ve mekân gözetmeden iletişim ve etkileşimine olanak sağlamış; diğer yandan da devletlerin iş yapış biçimlerini etkileyerek küresel ağa entegrasyonunu mümkün kılmıştır.

1990'ların ortasında ticari kullanıma açılmasıyla internet hızla yaygınlaşmış, bireysel kullanımın önemi ve sayısı artmıştır. Tüm dünyadaki kamular açısından internet özgürce iletişim kurabilecekleri bir alan olarak görülmüştür. Ancak siber uzama yönelik saldırılar ve kritik altyapıların uzama entegre edilmesi, beraberinde uzama devletlerin müdahil olmasını getirmiştir.

Siber uzamdan kaynaklanan ve uzama dışarıdan saldırılara karşı güvenliği sağlama kapsamında alınacak tedbirler, resmi politika belgeleriyle meşrulaştırılmıştır. Ancak belgelerle sadece güvenlik önlemleri değil, güvenlik önlemleri adı altında, bireysel hak ve özgürlüklerin kuşatma altına alınması ile, denetim, gözetim ve kontrol de meşrulaştırılmıştır. Bu durum düzenlemelerin, insanı merkez alan bir yaklaşımdan ziyade, devleti merkez alan bir yaklaşımın ürünü olmasından kaynaklanmaktadır. Ulusal, ekonomik ve kişisel güvenlik tedbirleri kapsamında siber uzama yönelik yapılan yasal düzenlemeler kişi hak ve özgürlüklerinde aşınmaya neden olmaktadır

Barack Obama yönetimi, siber uzam güvenliğini ABD için yüksek bir öncelik olarak tanımlayarak, uzamın militarizasyonunu hızlandırmıştır. ABD, liderlik temelli ve ulusal politikada öncelikli bir yaklaşım benimseyerek diğer ülkelerin de ABD'nin kurallarına uymasını sağlamayı amaçlamıştır. ABD'de uzama yönelik düzenlemeler yukarıdan aşağı ilerleyen bir düzeni beraberinde getirmektedir. AB politika metninde ise, uzamın güvenliğinin önemine vurgu yapılmakla birlikte, bireysel hak ve özgürlükleri de korunması gerektiği vurgulanmaktadır. Siber uzamın temel hak ve özgürlüklerin geliştiği bir alan olarak kullanılması eğilimi ağır basmaktadır.

AB belgelerinde güvenlikleştirme süreci daha tamamlanmamış ancak ciddi mesafe almıştır. Halihazırda gizlilik ve güvenlik arasındaki çatışmada gizliliğin temel olduğu, temel hak ve özgürlüklerin korunması gerektiği yaklaşımı hakimdir.

Türkiye'de siber uzama yönelik düzenlemeler bilgi toplumu söyleminin devamı olarak sunulsa da ABD söyleminden de etkilenen Türkiye siber güvenlik metninin, hibrit bir nitelik taşıdığı görülmektedir. Siber uzama yönelik güvenlik stratejisinin inşası ve sürdürülmesinde, kamu kurumları ve askeri kuruluşların yer alması, ülkedeki hâkim ulus devlet ve ulusal güvenlik söyleminin uzantısı olarak görülebilir. Ancak düzenlemelerin daha çok internete yönelik olması, internetin bireysel ya da toplu muhalif hareketlerin yeni ve farklı şekillerinin vücut bulduğu bir alan olması sonucunu doğurmuştur.

Kaynakça

Assange, J. (2013). *Şifrepunk: Özgürlük ve İnternetin Geleceği Üzerine Bir Tartışma*. Metis.

Banks, K. (2005). Index on censorship. *Summitry & Strategies,* 34(3), 85-91.

Barnard-Wills, D. (2013). Security, Privacy and Surveillance In European Policy Documents. *International Data Privacy Law*, 3, 170-180, doi: 10.1093/idpl/ipt014

Bazerman, C. (2003). Intertextuality: How texts rely on other texts. C. Bazerman, P. Prior (Ed). *What writing does and how it does It* içinde (s. 83-97). Lawrence Erlbaum Associates.

Beck, U. (2002). The terrorist threat: World risk society revisited. *Theory Culture Society*, 19(4), 39-55.

Beck, U. (2006). Living in the world risk society. *Economy and Society,* 35(3), 329-345.

Bendiek, A. (2014). Cybersecurity and civil liberties: A Task for the European Union. *Ethics and Armed Forces.* http://www.ethikundmilitaer.de/en/full-issues/20142-cyberwar/benediek-cybersecurity-and-civil-liberties-a-task-for-the-european-union/

Bendrath, R. (2001). The cyberwar debate perception and politics in U.S. critical infrastructure protection. *Information & Security: An International Journal,* 7, 80-103.

Bright, J. (2010). Security, technology and control: Repositioning securitisation theory for the information society. *Politics in Hard Times: International Relations Responses to the Financial Crisis.* SGIR

7th Pan-European Conference. https://www.mendeley.com/catalogue/ec490172-a857-3006-a23d-204b567f8688/

Burgess, J.P. (2007). Social values and material threat: the European programme for critical Infrastructure Protection. *International Journal of Critical Infrastructures*, 3(3-4), 471–487.

Burton, F. ve Carlen, P. (1979). *Official Discourse: On discourse analysis, government publications, ideology and the State.* Routledge & Kegan Paul.

Cavelty, M. D. (2008). *Cyber-security and threat politics*. Routledge.

Cavelty, M. D. (2012). The militarisation of cyberspace: Why less may be better. *4th International Conference on Cyber Conflict (CYCON 2012).* NATO CCD COE Publications, 141-152.

Cavelty, M. D. (2014). Global cyber-security policy evolution. *Cybersecurity in Switzerland*. Springer.

Clarke, R. A. ve Knake, R. K. (2011). *Siber savaş.* (M. Erduran, Çev.). İstanbul Kültür Üniversitesi Yayınları.

Çoban, S. (2013). *Teknolojik determinizm bağlamında bilgi toplumu strateji belgesinin incelenmesi.* Akdeniz Üniversitesi Akademik Bilişim Konferansı. https://ab.org.tr/ab13/bildiri/30.pdf

Deibert, R. J. ve Rohozinski, R. (2012). Contesting cyberspace and the coming crisis of authority. R. Deibert, J. Palfrey, R. Rohozinski ve J. Zittrain (Eds.) *Access contested: Security, identity, and resistance in Asian cyberspace* içinde (s. 21-42), MIT Press.

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. McClelland & Stewart.

Deisman, W. W. (2008). *Securing Cyberspace: Neo-Liberalism, risk and child safety*. [Yayımlanmamış doktora tezi]. Carleton University.

Denizcilik, U., & Bakanlığı, H. (2013). *Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı.* https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

Edmunds, D. and Wollenberg, E. (2001). A strategic approach to multistakeholder negotiations. *Development and Change*, 32(2), 231-253.

Elliott, R. (1996). Discourse analysis: Exploring action, function and conflict in social texts. *Marketing Intelligence & Planning*, 14(6), 65-68.

Fairclough, N. (1992). *Discourse and social change*. Polity.

Fairclough, N. (1995). *Critical discourse analysis: The critical study of language*. Longman.

Fairclough, N. (2001). *Language and power*. Pearson Education.

Fairclough, N. (2003*). Analyzing discourse: Textual analysis for social research*. Routledge.

Fiske, J. (2003). İletişim çalışmalarına giriş. (S. İrvan, Çev.). (2. Baskı). Bilim ve Sanat.

Foucault, M. (2002). Toplumu savunmak gerek. (Ş. Aktaş, Çev.). YKY

Giddens, A. (2000). *Elimizden kaçıp giden dünya*. (O. Akınhay, Çev.). Alfa Yayınları.

Grewal, B. S. (2008). *Neoliberalism and discourse: Case studies of knowledge policies in the Asia-Pacific.* [Yayımlanmamış doktora tezi]. Auckland University of Technology.

Hansen, L. (2006). *Security as practice: Discourse analysis and the Bosnian war*. Routledge.

Jackson, R. (2005). Writing the war on terrorism: Language. *Politics and Counterterrorism.* Manchester University Press.

Jager, S. (2001). Discourse and knowledge: Theoretical and methodological aspects of a critical discourse and dispositive analysis. R. Wodak & M. Meyer (Ed.) *Methods of Critical Discourse Analysis* içinde (s. 32-62). Sage.

JOIN/2013/01 final. (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace,* 7(1). http://ec.europa.eu/digital-agenda/en/cybersecurity.

Kabanov, Y. (2012). Information (Cyber-) security discourses and policies in the European Union and Russia: A comparative analysis. *Working*

Papers of Centre for German and European Studies. Centre for German and European Studies. https://publications.hse.ru/en/preprints/143476248

Karam, A. (2005). *Terror and patriotism in the United States: A critical analysis of governmental discourses surrounding the attacks of September 11, 2001 and the introduction of the Patriot Act in the United States of America* [Yayımlanmamış doktora tezi]. University of Ottawa.

Klingova, K. (2013). *Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia*. [Yayımlanmamış yüksek lisans tezi]. Budapest Central European University.

Krahmann, E. (2008). Security: Collective good or commodity? *European Journal of International Relations*, 14(3), 379-404.

Lawson, S. and Gehl, R.W. (2011). Convergence security: Cyber-surveillance and the biopolitical production of security. *Cyber-Surveillance in Everyday Life: An International Workshop.* https://www.robertwgehl.org/text/convergsec.pdf

Lawson, S. (2013). Motivating sybersecurity: Assessing the status of critical infrastructure as an object of cyber threats. *Cyber Behavior: Concepts, Methodologies, Tools, and Applications.* IGI Global, 168-189. doi: 10.4018/978-1-4666-2659-1.ch007

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Libicki, M. C. (2009). *Cyber deterrence and cyber war*. RAND Corporation.

Lyon, D. (2013). *Gözetim çalışmaları: Genel bir bakış*. (A. Toprak, Çev.). Kalkedon.

Manley, R. (2015). The fifth domain: Cyber-metaphors and apocalyptic rhetoric. *Brown Political Review*. https://brownpoliticalreview.org/2015/03/the-fifth-domain-cyber-metaphors-and-apocalyptic-rhetoric/

Mayasari, M., Darmayanti, N. and Riyanto, S. (2013). Critical discourse analysis of reporting on "Saweran for KPK Building" in media Indonesia Daily Newspaper. *International Journal of Linguistics*, 5(4), 213-224.

Neocleous, M. (2012). *Güvenlik, şiddet ve savaş*. (E. Embel ve G. Çorbacıoğlu, Çev.). Dipnot Yayınları.

Powers, S. M. ve Jablonski, M. M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University Of Illinois Press.

President, U. S. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. https://fas.org/irp/eprint/cyber-review.pdf

Raab, C. D. (2012, 2005). Governing the safety state. *Inaugural Lecture at the University of Edinburgh.* www.prescient-project.eu/prescient/ inhalte/download/5-Raab.pdf

Thee, M. (1977). Militarism and militarization in contemporary international relations. *Bulletin of Peace Proposal*, 8(3), 296-309.

Thibault, P. J. (1994). Intertextuality. R.E. Asher (Ed.) *The Encyclopedia of Language and Linguistics*. Pergamum Press, 4, 1751-54.

Tsui, C. (2014). *Tracing the discursive origins of the war on terror: President Clinton and the construction of new terrorism in the post-cold war era*. [Yayımlanmamış doktora tezi] University of Otago.

Ulmer, K. (2014). Cyber risks and Cyber security – risk communication and regulation strategies in the U.S. and Germany. *WorkinSWPBerlingPaper*. www.swp-berlin.org/fileadmin/ contents/products/arbeitspapiere/Ulm_WP_Cyber_Risks.pdf

Wagner, B. (2014). The politics of internet filtering: The United Kingdom and Germany in a comparative perspective. *Politics*, 34(1), 58–71.

Williams, R. (2003). *Televizyon, Teknoloji ve Kültürel Biçim.* (A.U. Türkbağ, Çev.). Dost Yayınları.

WSIS (2005). *WSIS Outcome Documents*. https://www.itu.int/net/wsis/ outcome/booklet.pdf.

Extended Abstract

Developments in information and communication technologies have eliminated time and space limitations in communication, it has enabled societies to meet new communication tools such as the Internet, wireless networks, mobile phones, and other communication media. The ways of doing business in the states have also changed with the developments in information and communication technologies. In addition to the positive effects and

opportunities these technologies create, they have also brought about private discussions. States' attempts to control cyberspace to protect their political influence and economic power have also become evident. Security-related issues and concerns have been instrumental in legitimizing control and surveillance attempts to extend new risk and threat definitions for the security of cyberspace.

The convergence between communication and security studies has also influenced the establishment and legitimation of security-related institutions, technologies, policies, and programs. Especially with the doctrine of a global war on terror led by the USA after the September 11, 2001 attacks the surveillance and control of information and communication technologies have been legitimized in the name of security. This study, it is aimed to reveal the strategies of legitimization of surveillance and control under the name of security measures for cyberspace, through the concepts of risk and threats. In this context, in the process of building a security discourse militarization towards cyberspace, legitimization of supervision, and surveillance activities are dealt with in interaction with public policies.

Discursive strategies that allow securitization are built through policy texts to regulate cyberspace. Policy texts are a means of publicizing official discourse and allow an ideological practice that legitimizes and legalizes the actions of the administration. At the same time, policy texts are the texts that enable us to understand how hegemony is developed, how different classes of society are included in the system, and thus the legitimacy of the state and the trust in the state are reinforced.

The main questions of the study are as follows:

- What kind of a construction process does the securitization discourse go through in cyberspace? How does this process affect people's rights and freedoms?

- Which discursive strategies are being implemented through the US, European Union (EU), and Turkey sample in this construction process?

In this context, the US, EU, and Turkey's cybersecurity policy documents were subject to critical discourse analysis. In Fairclough's critical discourse analysis, text analysis (verbal or written) as a whole includes the production, distribution, and consumption processes of the text (discourse practice) and the social dimension of the subject matter. In Fairclough's critical discourse analysis, a macro-level analysis is performed by focusing on the structuring of discourse order between different political domains. On the other two levels, meso and micro level, analysis takes place through text. The Meso-level analysis makes it possible to reveal discursive themes, strategies, and their connections with other texts.

In this study, the United States's "Cyber Space Policy Review (2009)", the EU's "Cybersecurity Strategy of the European Union: Open, Safe and Secure Cyberspace (2013)" "and Turkey's "National Cyber Security Strategy and 2013-2014 Action Plan "has been analyzed. Considering the widening of the scope of the regulations on cyberspace in a way that violates the rights and

freedoms of individuals, analysis of policy texts makes visible control and surveillance activities and ideological practices. As a result, the measures to be taken within the scope of ensuring security against attacks from outside and arising from cyberspace policy texts have been legitimized by official policy documents. This is because regulations are the product of a state-centered approach rather than a human-centered approach. The Barack Obama administration has accelerated the militarization of space by defining cyberspace security as a high priority for the US. The United States has taken a leadership-based and priority approach in national policy, aiming to make other countries abide by its own rules. In the USA, regulations for cyberspace bring a top-down order. In the EU policy text, the importance of the security of cyberspace is emphasized, as well as the need to protect individual rights and freedoms. The tendency to use cyberspace as an area where fundamental rights and freedoms are developed prevails. The securitization process in EU documents has not yet been completed, but it has taken serious progress. At present, privacy appears to be fundamental in the conflict between privacy and security. Fundamental rights and freedoms are seen as an area to be respected. Regulations for cyberspace in Turkey are presented as a continuation of the information society discourse. However, it also appears to be influenced by the US discourse. Turkey's cybersecurity policy document carries a hybrid nature.